Minimierung von Sicherheitsrisiken beim vernetzten Arbeiten im Gesundheitswesen

Minimierung von Sicherheitsrisiken beim vernetzten Arbeiten im Gesundheitswesen

Felix Gerdes, Cisco Systems GmbH

SchlieÃŸen Sie bei Auslandsreisen Ihren Reisepass vorm Verlassen des Hotels weg? Oder lassen Sie ihn auf dem Nachttisch liegen? Sicherlich fÃ¼hren Sie dieses nur mit erheblichem Aufwand zu ersetzende Dokument mit sich oder es wird â€“ trotz des beschrÃ¤nkt mÃ¶glichen Zutritts zum Hotelzimmer â€“ zusÃ¤tzlich unter Verschluss gebracht. So mache ich e jedenfalls â€“ angepasst an den Risikograd. In manchen Situationen erscheint ein abgeschlossener Koffer als Aufbewahrungsort als ausreichend sicher. In einem Land hatte ich jedoch auch bei der Aufbewahrung im Hoteltresor kein sehr gutes GefÃ¼hl. Wir passen fast immer unsere eigenen SicherheitsmaÃŸnahmen intuitiv den gegebenen Situationen an.

Patientenakten, sofern sie noch in Papierform existieren, werden ebenso spÃ¤testens am Ende des Tages unter Verschluss gebracht. So hofft man zumindest. TagsÃ¼ber werden Akten, die gerade gebraucht werden, nicht vÃ¶llig unbeaufsichtigt offen liegen gelassen. Ã„rzte, Schwestern und Arzthelfer verringern das Risiko der Einsicht durch Unbefugte oder den Diebstahl der Akte durch ihr Handeln. Sie passen ihr Handeln am Arbeitsplatz, sei es in der Praxis oder in der Klinik, der RisikoeinschÃ¤tzung an. Die Anweisungen zum sicheren Umgang mit Patientendaten, die die Mitarbeiter erhalten, beruhen auf formal oder weniger formal und intuitiv durchgefÃ¼hrten Bedrohungsanalysen: â€žLiegt diese Akte hier sicher ? Merken ich oder meine Mitarbeiter es, falls die Akte verschwindet? Ist der Zugang von Patienten in diesem Bereich eingeschrÃ¤nkt und kontrolliert?â€œ

Nun werden bald, dank der elektronischen Gesundheitskarte, Patientendaten elektronisch kommuniziert. Die EinfÃ¼hrung des elektronischen Rezepts bedeutet fÃ¼r eine Praxis oder Apotheke ein Wechsel von Papier auf elektronische Versandmedien. Der Zugang zum Gesundheitsnetzwerk erfordert daher eine neue RisikoeinschÃ¤tzung. Das neue, vernetzte Arbeiten im Gesundheitswesen, von dem wir uns alle QualitÃ¤tsprÃ¼nge und Kosteneinsparungen erhoffen, verlangt, dass jeder, der einen Heilberuf ausÃ¼bt und jedes Krankenhaus, jede Krankenversicherung, jede Apotheke und jedes zuliefernde Rechenzentrum sich zu Beginn der EinfÃ¼hrung der elektronischen Gesundheitskarte Gedanken Ã¼ber die Risiken dieser neuen Arbeitsweise macht.

Vernetztes Arbeiten ist nicht per se risikoreicher als das Arbeiten ohne Netzzugang. Es wird generell sogar davon ausgegangen, dass trotz des vernetzten Arbeitens, Patientendaten noch sicherer bearbeitet, versendet und gespeichert werden. Um diesen Sicherheitsgrad zu erreichen, bedarf es jedoch, dass Teilnehmer am Gesundheitsnetzwerk ihre Arbeitsweise â€“ bestimmte AblÃ¤ufe und organisatorische Aspekte des tÃ¤glichen Handelns â€“ den neuen Medien anpassen.

Neue Technologien haben schon immer eine Anpassung unseres Handelns erforderlich gemacht

Genau wie der Computer mehr ist als eine Schreibmaschine, so ist das Gesundheitsnetzwerk viel mehr als ein Ersatz fÃ¼r Faxverkehr oder den Transfer von Daten per Diskette. Es wÃ¤re also ein Trugschluss zu glauben, man mÃ¼sste seine AblÃ¤ufe in der Praxis, der Apotheke oder in der Klinik kaum anpassen. Die Adoption von neuen Technologien (beispielsweise das Automobil, EC-Karten oder das Mobiltelefon) erfordert immer ein gewisses Umdenken und das Anpassen des eigenen Handelns in Zusammenhang mit der Technologie. Bei dieser Adoption einer neuen Technologie passen wir uns unbewusst oder bewusst und systematisch den neuen Gegebenheiten an. Die hohe Bedeutung, die dem Schutz von vertraulichen Patientendaten beigemessen wird, spricht dafÃ¼r, dass Teilnehmer am Gesundheitsnetzwerk sich ebenfalls bewusst und systematisch auf die neue Arbeitsweise vorbereiten. Die notwendigen Vorkehrungen mÃ¼ssen weder verhÃ¤ltnismÃ¤ÃŸig teuer noch mit persÃ¶nlichen Nachteilen verbunden sein. Konsequent durchgefÃ¼hrt bieten sie einen umfassenden Schutz vor Verlust von Patientendaten sowie unbefugtem Zugang zum Gesundheitsnetzwerk.

Die zu treffenden SicherheitsmaÃŸnahmen sollten aktuellen Risiken angemessen sein. Gleichzeitig sollten die KomplexitÃ¤t sowie der Aufwand dieser MaÃŸnahmen handhabbar bleiben. Sowohl GroÃŸkliniken als auch kleinere Arztpraxen und Apotheken haben es mit Risiken durch Bedrohungen, Diebstahl, Verlust und BetriebsausfÃ¤lle zu tun.

Vor einigen Jahren hatte ein Systemadministrator noch Wochen oder Tage Zeit, um GegenmaÃŸnahmen gegen Netzwerkbedrohungen einzuleiten. Das Zeitfenster fÃ¼r solche MaÃŸnahmen hat sich heute auf Minuten oder Sekunden verringert. Der Internet-Wurm â€žSapphireâ€œ hatte im Januar 2003 nur 11 Minuten gebraucht, um sich weltweit zu verbreiten und einen immensen Schaden anzurichten. Das Herunterladen von Virenschutz-Updates kann daher nicht mehr die einzige SchutzmaÃŸnahme fÃ¼r Netzwerke und EndgerÃ¤te sein. ...

Dokumentinformationen zum Volltext-Download
Â
Titel:
Minimierung von Sicherheitsrisiken beim vernetzten Arbeiten im GesundheitswesenArtikelÂ istÂ erschienenÂ in:
TelemedizinfÃ¼hrer Deutschland, Ausgabe 2006
Kontakt/Autor(en):Felix Gerdes, Cisco Systems GmbH Seitenzahl:
3,5 Sonstiges:

keine Abb. Dateityp/ -grÃ¶ÃŸe: PDF / 499Â kBÂ Click&Buy-PreisÂ inÂ Euro: 0,00

Â Rechtlicher Hinweis: